(Rev.8/82)

ANTICIPATORY SEARCH WARRANT ON WRITTEN AFFIDAVIT

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. THE PREMISES KNOWN AS: The residence or vehicle in which the beeper in an International DHL Mail Service package with tracking number EM240573736IN, addressed to Nasser Abyaneh Ghadiri, with a delivery address of 22704 Ventura Blvd, #428, Woodland Hills, California 91364, indicates the device has been activated or visual surveillance indicates the package has been opened	DOCKET NO. MAGISTRATE'S CASE NO. 2:23-MJ-03333 TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

Affidavit having been made before me by the below-named affiant that he/she has reason to believe that on the premises known as

SEE ATTACHMENT A

in the Central District of California

there will be concealed certain property, namely:

SEE ATTACHMENT B

and as I am satisfied that there is probable cause to believe that upon the occurrence of the triggering circumstances described in Section VI of the search warrant affidavit, the property so described will be concealed on the person or premises above-described and the grounds for application for issuance of the search warrant exist as stated in the supporting affidavit which is incorporated herein by reference.

YOU ARE HEREBY COMMANDED to search on or before fourteen (14) days (not to exceed 14 days) the person or place named above for the property specified, serving this warrant and making the search at any time in the day or night upon the occurrence of the event described above, and if the property be found there to seize it, leaving a copy of this warrant and receipt for the property taken, and prepare a written inventory of the property seized and promptly return this warrant to the duty U.S. Magistrate Judge as required by law.

NAME OF AFFIANT	SIGNATURE U.S. MAGISTRATE JUDGE**	DATE/TIME ISSUED
Jerome S. Salvador, Special Agent, Homeland Security Investigations	The Honorable Charles Eick	

AUSA: Derek R. Flores x4896

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PROPERTY TAKEN PURSUANT TO THE WARRANT

CERTIFICATION

I swear that this inventory is a true and detailed account of all the property taken by me on the warrant.

_____

Subscribed, sworn to, and returned before me this date.

_____ _____

U.S. JUDGE OR MAGISTRATE **DATE**

ATTACHMENT A

PREMISES TO BE SEARCHED

The SUBJECT PREMISES to be searched is defined as the residence or vehicle at which the BEEPER in an International DHL Mail Service package with tracking number EM240573736IN, addressed to Nasser Abyaneh GHADIRI, with a delivery address of 22704 Ventura Blvd, #428, Woodland Hills, California 91364, indicates the device has been activated or visual surveillance indicates the package has been opened.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband fruits, or instrumentalities of violations of 18 U.S.C. § 542 (Entry of Goods by Means of False Statements), 18 U.S.C. § 545 (Smuggling Goods into the United States), 21 U.S.C. § 841 (Distribution of and Possession with Intent to Distribute a Controlled Substance), 21 U.S.C. § 846 (Attempt and Conspiracy to Commit a Controlled Substance Offense), and 21 U.S.C. § 952 (Importation of Controlled Substance) (collectively, the "SUBJECT OFFENSES"), namely:

a. The SUBJECT PACKAGE, an DHL package with tracking number 7579278136 addressed to Nasser GHADIRI, 22704 Ventura Boulevard # 428, Woodland Hills, California 91364, and its contents, including the following:

i. Approximately one (1) box, containing approximately three (3) metal cylinders;

ii. A Global Positioning System tracker or beeper device used to signify that the SUBJECT PACKAGE has been opened; and

iii. The packing effects used to package and ship the SUBJECT PACKAGE;

b. Any controlled substance, controlled substance analogue, or listed chemical;

c. Any parcels from any address or company in Oman;

d. Data, records, documents, programs, applications or materials relating to the trafficking of controlled

substances, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when controlled substances were bought, sold or otherwise distributed and any materials, documents, or records that are related to the sale, purchase, receipt, or possession of any controlled substance, including books, receipts, photographs, bills of sale, shipping receipts, identification cards, bank statements, and correspondence discussing, requesting or confirming purchase, sale or shipment;

e. Tools, paraphernalia, or materials used as a means of packaging, selling, or distributing controlled substances, to include: scales and other weighing devices, packing materials, plastic baggies, heat- and vacuum-sealing devices, vials, and balloons;

f. Any indicia of occupancy, residency, or ownership of the SUBJECT PREMISES and things described in the warrant, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

g. Items of personal property reflecting names, addresses, telephone numbers, or communications of members or associates involved in controlled substance trafficking activities, including personal telephone books, address books, telephone bills, photographs, videotapes, facsimiles, personal

notes, cables, telegrams, receipts, and documents and other items;

h. Any bills and/or subscriber documents related to digital devices used to facilitate the SUBJECT OFFENSES;

i. United States currency, money orders, or similar monetary instruments over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds);

j. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, rubber bands, plastic or shrink wrap, and plastic sealing machines;

k. Records, documents, programs, applications, or materials reflecting or relating to payment, receipt, concealment, transfer, or movement of money, including but not limited to bank account records and other financial institution records, wire transfer records, receipts, safe deposit box keys and records, and notes;

l. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

m. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any digital devices used to facilitate the SUBJECT OFFENSES and all telephone numbers

accessed through any push-to-talk functions, as well as all received or missed incoming calls;

n. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email or social media communications or other text or written communications sent to or received from any digital device;

o. Contents of any calendar or date book, including any calendars or date books stored on any digital devices;

p. Audio recordings, photographs, video recordings or still captured images on any digital device, phone memory cards, or other storage related to the purchase, sale, transportation, or distribution of controlled substances and listed chemicals or the collection, transfer or laundering of the proceeds of illegal activities;

q. GPS coordinates and other location information or records identifying travel routes, destinations, origination points, and other locations;

r. Any digital device used to facilitate the above listed violations and forensic copies thereof.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

6. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to

be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel

assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.